REMARKS

Claims 1-19 are pending in the Application.

Claims 1-18 stand rejected.

Claim 19 has been allowed.

I. REJECTIONS UNDER 35 U.S.C. § 101

Claims 10-17 stand rejected under 35 U.S.C.§ 101. The Examiner has suggested that the word "adaptable" makes the limitations optional for storage on a computer readable medium. In response, Applicants have amended these claims to remove the word "adaptable."

II. REJECTIONS UNDER 35 U.S.C. § 102

Claims 1-3, 7-12 and 16-17 stand rejected under 35 U.S.C. § 102(e) as being anticipated by *Alexander et al.* (U.S. Patent No. 6,188,602). Since these claims have been amended, these rejections are moot.

III. REJECTIONS UNDER 35 U.S.C. § 103

Claims 4-6, 13-15 and 18 stand rejected under 35 U.S.C. § 103 as being unpatentable over *Alexander* in view of *Grawrock* (U.S. Patent No. 6,678,833). In response, Applicants respectfully traverse these rejections.

The Examiner is attempting to combine *Grawrock* and *Alexander* in an impermissible manner. Nothing within *Alexander* teaches or suggests a need or even a hint for using a TPM such as taught in *Grawrock.*

The Examiner asserts that the motivation to combine the two references is provided in *Grawrock* at column 2, lines 1-6. *Grawrock* teaches that the TPM is bound physically or logically to the boot block memory device, such as shown in Figure 2 of *Grawrock*. This resulting configuration, allows the TPM to accurately report the identity of the boot block without reliance on any intervening devices. Though a combination of *Grawrock* and *Alexander* may suggest that a TPM can be used to verify the identity of a boot block code, it does not suggest an ability to use a TPM to verify and update to such a boot block code, or especially a BIOS utility, such as recited in some of the claims. In fact, *Grawrock* teaches away from the present invention by specifically stating that it uses the TPM so that there is no reliance on any intervening devices, while the present invention uses such an intervening device through the utilization of the SMI handler to query a status of the verifying step. In other words, *Grawrock* has the TPM so physically or logically connected to the boot block memory unit so that it does not require such utilities as an SMI handler to assist it in verifying updates that may be desired to be stored on such a memory unit.

With respect to claims 5 and 14 the Examiner asserts that the combination of *Alexander* and *Grawrock* would teach that an SMI handler could be used to query the status of the verifying step by querying the TPM for such status. The Examiner cites *Grawrock*, column 4, lines 1-9. This language in *Grawrock*, however, teaches that the TPM can be used to perform a hash operation on various software modules to produce an identifier that is then stored within the TPM, and then can be used to later respond to challengers wanting to verify the authenticity of such software modules. Column 3, line 50 - column 4, line 18. What is important is that the combination of these two references does not teach or suggest that an update to one of these software modules, and specifically the BIOS (as recited in several of the claims), is performed by the TPM before an update of such software module is accomplished. *Grawrock* teaches verification after it has already been loaded onto the system, whereas the present invention teaches a way to verify the BIOS is unaltered before allowing it to be flashed onto the system. This is the same difference as between catching the criminal after the crime has been committed versus preventing the crime.

With respect to claims 6 and 15, the Examiner has asserted that the combination of *Alexander* and *Grawrock* teaches the SMI handler being issued by the TPM. This is in no way suggested by these two combinations. The Examiner cannot make such an assertion without attempting to at least prove it with some logical reasoning. The Examiner's assertion on page 5 of the Office Action is merely an unsupported single-sentenced statement.

With respect to claim 18, the foregoing arguments also apply.

IV. CONCLUSION

As a result of the foregoing, it is asserted by Applicants that the remaining Claims in the Application are in condition for allowance, and respectfully request an early allowance of such Claims.

Applicants respectfully request that the Examiner call Applicants' attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining problems.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicant

By: _____
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851